MORRISON & FOERSTER LLP
Jamie A. Levitt
Damion K.L. Stodola
1290 Avenue of the Americas
New York, NY 10104-0050
(212) 468-8000
Attorneys for Plaintiff Verified Identity Pass, Inc.

Of Counsel
Lori A. Schechter
MORRISON & FOERSTER LLP
425 Market Street
San Francisco, California 94105-2482
(415) 268-7000

UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

VERIFIED IDENTITY PASS, Inc., d/b/a CLEAR REGISTERED TRAVELER, Plaintiff, -against- FRED FISCHER, SAFLINK CORPORATION, and FLO CORPORATION, Defendants.	No. 07 Civ. ___

MEMORANDUM OF LAW IN SUPPORT OF VERIFIED IDENTITY PASS, INC.'S REQUEST FOR A TEMPORARY RESTRAINING ORDER AND PRELIMINARY INJUNCTION

TABLE OF CONTENTS

TABLE OF AUTHORITIES

CASES

STATUTES

MISCELLANEOUS

Pursuant to Rule 65 of the Federal Rules of Civil Procedure ("Fed. R. Civ. P.") plaintiff Verified Identity Pass, Inc. ("Verified" or the "Company") respectfully submits this memorandum of law in support of its application for a temporary restraining order and a preliminary injunction to enjoin its former employee, defendant Fred Fischer, and his current employers, Verified's direct competitors, defendants FLO Corporation ("FLO") and Saflink Corporation ("Saflink"), from, among other things, their misappropriation and unscrupulous competitive use of Verified's trade secrets.

PRELIMINARY STATEMENT

Fred Fischer, after being terminated, and in his last hours of employment as the Senior Vice President of Sales at Verified, logged into Verified's computer system from a remote computer and downloaded the entire annotated contact list from Verified's highly confidential and proprietary Salesforce Database. He then went to work for Verified's direct competitor, FLO[1], and proceeded to use that contact list to solicit the key contacts from Verified's database for the benefit of FLO. This, however, was only the tip of the iceberg. Indeed, since his termination, Fischer had made numerous attempts to hack into Verified's systems, and has disparaged Verified and disclosed its confidential and proprietary information to airport officials. Defendants' web of misconduct began to unravel when on July 10, 2007, they sent a mass e-mailing to the contacts on Verified's database, which happened to include several contacts whom FLO would have no legitimate basis to solicit – including a good friend, and the maid-of-honor, of one of Verified's Senior Vice Presidents.

Verified operates in the extremely sensitive field of airport security. It is the leading approved service provider operating the Transportation Security Administration's Registered

[1] For convenience, unless otherwise noted, "FLO" is used to refer to both FLO and its parent company Saflink.

Traveler Program, a pre-screening program in which qualified passengers may use special expedited security lines at participating airports across the country. FLO has attempted to compete with Verified in this industry.

When Fischer joined FLO, he was armed with one of Verified's most important assets -- the contacts and related information from the Salesforce Database he stole -- which contains valuable confidential and proprietary information used to keep track of business contacts, partners, prospective partners, prospects, the status of contracts, and other sensitive information, including confidential notes and comments regarding negotiations and other business dealings. Despite his employment agreement in which he agreed to "keep such information strictly confidential" for five years following his termination from Verified, Fischer and FLO used this information, as well as other information Fischer obtained as a key executive of Verified, in an effort to gain an unfair competitive advantage for FLO.

FLO knew that Fischer's competitive tactics were unscrupulous. In fact, any question there could have been that FLO was aware of Fischer's misconduct was removed when Verified and FLO settled prior litigation between the parties, well before FLO used Verified's confidential database information. At that time, FLO's president directly recognized that Fischer was "an unguided missile" and promised to "control him." Yet, they did not. On the same day as the parties were having settlement discussions, Fischer, as he had done on several prior occasions, tried to hack into Verified's system. Indeed, on July 10, 2007, after Verified first got wind of the mass e-mailings going to its database, Verified's CEO called FLO's president and left two voice mails, one of which directly referenced Fischer and his misconduct, and urgently requested a return call. But, instead of a return call, less than a week later, on July 16th, another mass e-mailing went out to Verified's contacts "on behalf of FLO."

Fischer's conduct is not only a breach of the continuing obligations under his employment agreement, but defendants have violated the federal Computer Fraud and Abuse Act, and various state laws, including the misappropriation of Verified's trade secrets. This conduct is ongoing and injunctive relief is necessary to prevent further immediate and irreparable harm to Verified resulting from the use and disclosure of its protected trade secrets, and to prevent future attempts to hack into its computer system.

STATEMENT OF FACTS

A. Verified is the Pioneer for the Registered Traveler Program

Verified is the leading approved service provider currently operating the Registered Traveler Program of the Transportation Security Administration ("TSA"). (Affidavit of Steven Brill, dated July 18, 2007 ("Brill Aff."), at ¶ 2.) The TSA's Registered Traveler Program is a pre-screening program. Qualified passengers who pass a security background check conducted by the TSA receive a biometric card that allows them to use special expedited security lines at airports across the country that participate in the program. Airports and airlines are allowed by TSA to choose a service provider to operate the program at airports and airline terminals, whereupon that service provider constructs and staffs the special Registered Traveler lanes and enrolls travelers, who are charged an annual subscription fee. (*Id.*)

Verified was chosen to operate the first private sector Registered Traveler Program in the United States. (*Id.* at ¶ 3.) Since that time, based upon its experience and its strong customer service record, Verified has been selected as the Registered Traveler service provider by every airport that has chosen a provider in a competitive bidding process. Verified currently has contracts with several airlines at JFK, with Air Tran Airways at La Guardia, and with Virgin Atlantic at Newark Airport, as well as contracts with the Albany, San Jose, Indianapolis, Cincinnati, Westchester County, and Orlando Airports. In addition, Verified has signed a

contract with the San Francisco Airport to begin a program there in September. (*Id.*) Except for a program run by the Unisys Corporation at the Reno Airport, there are no other companies currently operating the Registered Travel lanes any airport in the United States. (*Id.*) Defendant Saflink, which now operates under the name of FLO, also competes with Verified but so far has never been chosen to operate a program by any airport or airline nor enrolled a single customer in a Registered Traveler program. (*Id.*)

B. Fischer was a Key Executive for Verified with Access to Plaintiff's Most Sensitive Trade Secrets

Fischer was hired for the position of Senior Vice President of Sales for Verified, commencing on December 5, 2005. (*Id.* at ¶ 4; Affidavit of Allison Beer, dated July 19, 2007, ("Beer Aff."), at ¶ 6.) He was responsible for corporate sales and strategic partnerships as well as Verified's efforts to sell bulk employee memberships in the Registered Traveler program to major corporations and for arranging co-marketing partnerships with major travel industry companies, such as rental car companies and hotel chains, and corporate travel management companies. (Brill Aff. at ¶ 4; Beer Aff. at ¶ 6.) In that position, Fischer was exposed to a great deal of Verified's most sensitive, proprietary and confidential information, particularly having to do with its pricing, marketing strategies, and corporate business contacts, partners and customers. (Brill Aff. at ¶ 4; Beer Aff. at ¶¶ 5-7.)

Verified zealously maintained and secured its intellectual property, and Fischer agreed to do the same on Verified's behalf. Thus, Fischer signed an employment agreement and acknowledged that "as a key executive of the company" he would "be privy to the company's trade secrets, customer accounts, business practices and other proprietary information" and agreed "to keep such information strictly confidential for a term of five years following" the termination of his employment. (*Id.* at ¶ 5; Brill Aff., Ex. A ("Employment Agreement").)

Fischer also agreed to abide by all of the provisions of Verified's employee handbook, "including but not limited to, [Verified's] strict policies and practices with regard to the protection of the privacy of [its] customer accounts." (Brill Aff., Ex. A at 2.) The employee handbook provided to Fischer, expressly states that Verified "regard[s its] business plan, customer lists, published documents and internal work product to be proprietary and confidential" and "will fire anyone who reveals any of this without authorization." (Brill Aff. at ¶ 6; Ex. B ("Employee Handbook") at 22.)

Verified took additional steps to secure the confidentiality of its most proprietary information by limiting access within the Company. During his employment, Fischer also was one of only seven senior employees who had access to Verified's extremely sensitive and proprietary Salesforce Database ("Database").[2] (Brill Aff. at ¶ 7; Beer Aff. at ¶ 7.) The Database is an electronic database that contains highly sensitive confidential and proprietary information used by Verified's senior sales executives to keep track of business contacts, partners, prospective partners, the status of contracts and negotiations, and other information. (Brill Aff. at ¶ 7.) The data contained in the Database was compiled based upon the significant efforts of multiple Verified employees over multiple years to establish contacts and potential business relationships. (*Id.*) This data includes information that is not readily ascertainable, such as names and contact information for key decision makers at airports across the country, at major travel companies who have or might become Verified's strategic partners, and at major corporations who purchase travel services for their companies' employees. (*Id.*) The Database also contains personal information for these contacts, as well as sensitive and confidential notes, comments, and other information regarding negotiations, deals, and the status of such, all of

[2] Since Fischer's termination from Verified, only three other individuals have been granted access to the database. (Beer Aff. at ¶ 7.)

which is essential for the growth and development of Verified's business and little of which could be known to others outside the Company. (*Id.*)

Because the Registered Traveler field is still a relatively new, emerging field, airports and key travel industry players (such as airlines, hotel chains, rental car companies, and credit card providers) are right now making key decisions about alliances that will shape the industry and affect the fortunes of companies like Verified for years to come. (*Id.* at ¶ 8.) Registered travel is all that Verified does, and being able to compete fairly in this environment is crucial to Verified's survival and success. (*Id.*)

Consequently, Verified is keenly aware of the need to protect its confidential information. In addition to securing confidentiality agreements, securing employees' compliance with the Employee Handbook, and limiting access, Verified's highest levels of management routinely reminded those individuals with access to the Database that it contained confidential and proprietary information, and that it was crucial to Verified's business success that they take special care to maintain the confidentiality of this information. (*Id.*; Beer Aff. at ¶ 9.) Fischer was included among this group, and Verified's CEO specifically recalls communicating with him on the subject of Verified's confidential information. (Brill Aff. at ¶ 8.)

Verified also secured the Database by limiting the ability to access or edit information on the Database through a password protected Verified terminal or through a password protected website. (Beer Aff. at ¶ 8.) Verified kept an electronic log of all attempts to access the Database, whether successful or unsuccessful. (*Id.*; Beer Aff., Ex. A (excerpts of log).)

C. Fischer Steals Contacts Within the Salesforce Database

In late November 2006, Fischer was informed that his employment was terminated and that his last day would be December 5, 2006. (Beer Aff. at ¶ 10; Brill Aff. at ¶ 9.) Yet, in the last hours of his employment, Fischer logged into Verified's computer systems remotely from a

computer out of the office, and intentionally downloaded portions of the Database, including confidential and valuable contact information into an Excel spreadsheet on his computer. (Brill Aff. at ¶ 10; Beer Aff. at ¶ 10, Ex. B (electronic profile); Affidavit of Alan Brill, dated July 19, 2007 ("Kroll Aff."), at ¶¶ 15-19.) This access to Verified's computer systems and download was unauthorized and exceeded any authorized access Fischer had to Verified's computer systems. (Brill Aff. at ¶ 10.)

Shortly thereafter, Fischer began working for Verified's competitor, FLO Corporation. (Brill Aff. at ¶ 11; Beer Aff. at ¶ 11.) FLO Corporation directly competes with Verified in seeking to obtain contracts to operate the Registered Traveler program at airports across the United States, including in the bid for the Registered Traveler program for the Little Rock Municipal Airport, in Little Rock Arkansas. (Brill Aff. at ¶ 12.) FLO also competes with Verified in the sale of memberships in registered traveler programs to corporate travel departments, employers and other individuals who then become eligible for biometric cards that allow travelers to use the special expedited airport security lanes at various airports. (Brill Aff. at ¶ 13.) Saflink, the parent company of FLO, issued a press release on March 26, 2007, announcing that Fischer had been appointed as "Senior Vice President, Strategic Sales," and would be responsible for sales of the "FLO Registered Traveler (RT) program to corporations, travel management companies, airlines, credit cared companies and retail partners." (*Id.* at ¶ 14.)

Since Fischer commenced employment as a senior executive at FLO, he has repeatedly attempted to interfere with Verified's efforts to lawfully compete for airport contracts and memberships in its Registered Traveler Program by, among other things, disparaging Verified and using Verified's proprietary and confidential information, all of it learned by Fischer during his employment and much of it retrieved unlawfully on his last day at Verified, to advantage FLO and Saflink, his new employer.

D. Fischer Disparages Verified To Airports

On February 23, 2007, the Little Rock Airport Commission (the "Commission") issued a request for proposals seeking to implement a Registered Traveler program at the Little Rock Municipal Airport. (Brill Aff. at ¶ 16.) Verified submitted its proposal in response to the RFP. (*Id.*) FLO also submitted a proposal for the Little Rock Registered Traveler program on March 28, 2007 just two days after Fischer joined FLO. (*Id.*) The Little Rock RFP stated that the bids would be publicly opened, and Verified obtained a copy of FLO's Little Rock Proposal from the Commission based upon a routine Freedom of Information Act request. (*Id.*)

Each of the three bidders in Little Rock was invited to, and in fact did, deliver an oral presentation to members of the Commission at a public meeting on April 11, 2007. (*Id.* at ¶ 17.) The oral presentations were recorded by the Commission. Fischer participated in FLO's oral presentation to the Commission. (*Id.*) During FLO's presentation, Fischer, in violation of his employment agreement, referenced confidential and proprietary information he learned while employed as a Senior Vice President at Verified. (*Id.* at ¶ 18) For example, Fischer told the Commission:

- About Verified's revenue sharing formula and method, prefacing his comment with this introduction: "As far as I know from working for our competitor…" (Tr. at p. 30 & pp. 17-18);
- About how corporate travel managers regard the idea of reimbursing employees for a Registered Traveler card, prefacing those remarks with the reminder that he came "to FLO from Verified Identity" where he had "seen over 250 corporate travel managers across the country" of which "only two said they wouldn't reimburse for the card" (Tr. at p. 26);

- About Verified's terms and conditions for setting up mobile enrollments at corporations, declaring that the Commission will "hear from our competitors" that they will only set up remote kiosks to sign up customers for the Registered Traveler Program, if a company will have a minimum of 250 people to enroll. (Tr. at p. 35).

(*Id.* at ¶ 18; Ex. D (transcript excerpts).)

On or about, April 18, 2007, Verified was notified that it had been awarded the contract for the Little Rock Registered Traveler program. (Brill Aff. at ¶ 19.) After learning that it did not get the contract, FLO requested a debriefing from the Commission. (*Id.*) On April 23, 2007, representatives for FLO, including Fischer, had a telephone conference with Ronald Mathieu, the Little Rock National Airport's Deputy Executive Director, to debrief the Commission as to why FLO was not selected as the winning bidder. (*Id.* at ¶ 20.) Among other things, after Fischer stated that he had come from Verified, he indicated that he was "number three" there, and that Verified falsely represented the number of its card holders. He also asserted that Verified's biometric cards are "not interoperable" and "the program is not even interoperable in their own company." These statements are completely false. (*Id.* at ¶ 21, Ex. E (transcript of April 23 call).)

E. FLO's Knowledge of Fischer's Unscrupulous Competitive Tactics

After the April 23, 2007, phone conference with Mr. Mathieu, FLO filed a protest with the Commission, asserting that bidding process had been compromised because the Commission provided Verified with access to FLO's Little Rock Proposal, in response to Verified's FOIA request. (*Id.* at ¶ 22.) On May 29, 2007, the Commission notified FLO that its protest would be denied. (*Id.*)

FLO then filed a lawsuit against Verified in California Superior Court, in San Francisco (the "California Action"), alleging that Verified stole its trade secrets based upon the

Commission's disclosure of FLO's proposal in response to the FOIA request. (*Id.* at ¶ 24.) After failing to get a restraining order in the California Action, on June 4, 2007, FLO filed a second lawsuit, in the United States District Court for the Eastern District of Arkansas (the "Arkansas Action"), against the Commission, seeking to enjoin the Commission from awarding the contract to Verified. (*Id.* at ¶ 25.) Verified was granted the right to intervene in the Arkansas Action as a matter of right. (*Id.*)

On June 12, 2007, a hearing was held in the Arkansas Action, and the court dismissed FLO's case on jurisdictional grounds. (*Id.* at ¶ 26.) After this hearing, Verified's CEO met with Glenn Argenbright, FLO's President, who was clearly concerned that Verified was seeking reimbursement for all legal fees resulting from these groundless lawsuits. (*Id.*) Verified subsequently agreed not to seek legal fees from FLO under California's trade secret statute for FLO's bad faith litigation in return for FLO ceasing all such litigation and acknowledging that Verified's conduct has been lawful and honorable at all times. (*Id.*) Specifically, the parties agreed to cessation of the California Action and the Arkansas Action with a dismissal with prejudice by FLO of all claims alleged against Verified in the California Action, no payment of money by Verified, and a waiver by FLO of all appeal rights from the dismissal of the Arkansas Action. (*Id.*) Over the next day the parties finalized the settlement and on June 14, 2007, a settlement agreement was signed. (*Id.*, Ex. G (Settlement Agreement))

As a result of the proceedings in the California and Arkansas Actions, FLO was put on notice, if it was not previously aware, of the conduct of Fischer, while acting in his capacity as Senior Vice President for FLO. (*Id.* at ¶ 27.) Saflink and FLO senior management reviewed the transcript of statements made by Fischer during the April 11 Hearing and the audio tape of Fischer's comments in the April 23 telephone conference. (*Id.*) FLO's president, Mr.

Argenbright, even apologized for. Fischer's misconduct and said that Fischer "was sometimes an unguided missile" and promised that FLO would "control him." (*Id.*)

F. Fischer Attempts to Hack into Verified's Computer Systems to Benefit Defendants

In addition to stealing Verified's confidential information the day he left Verified's employ, forensic analysis shows that Fischer, while employed at FLO, tried to hack into Verified's computer systems on eight separate occasions. Log files demonstrate that Fischer, from a computer in North Carolina, attempted to access the Salesforce Database on January 31, 2007, April 6, 2007 (during the Little Rock bidding process), June 12, 2007, the very evening that FLO and Verified were negotiating the settlement of the California and Arkansas Actions, in which Mr. Fischer's wrongful conduct was a significant issue, and June 29, 2007. (Brill Aff. at ¶ 34; Beer Aff. at ¶ 12; Kroll Aff. at ¶ 21.) He also attempted to log into another Verified computer system on four occasions on February 20, 2007. (Kroll Aff. at ¶ 22.)

It has now become apparent that defendants are using the contact and other information Fischer stole from the Salesforce Database on his last day at Verified to solicit business for FLO with several mass e-mailings to Verified's contacts. (Brill Aff. at ¶ 28.) Defendants first sent an e-mail to contacts in the Salesforce Database in early July, giving them an opportunity to opt-out of Saflink's mailing list. (*Id.*; Beer Aff. at ¶ 14; Ex. C) A week later, on July 10, 2007, defendants sent these same persons an e-mail advertisement offering a 35% discount if they entered into "a non-binding letter of intent" with Saflink by July 20, 2007, and advising them to contact Fred Fischer at FLO Corporation. (Brill Aff. at ¶ 28; Beer Aff. at ¶ 15, Ex. D) Several of the recipients contacted Verified surprised to have received this unsolicited offer. (Brill Aff. at ¶ 27; Beer Aff. at ¶ 18.)

On July 10th, upon learning of these e-mails that were sent to the contacts in the Salesforce Database , Verified's CEO immediately called FLO President Glen Argenbright and left him two messages, one which referenced Fischer's misconduct, and both urging him to return the call. (Brill Aff. at ¶ 32.) Mr. Argenbright has not returned any calls. (*Id.* at ¶ 33.)

Instead, the following week, on July 16, 2007, FLO sent yet another mass e-mail to contacts from Verified's Salesforce Database requesting that its recipients participate in a 7-minute survey "regarding several aspects of the [registered travel] program that the Business Travel Coalition is conducting on behalf of FLO Corporation." (Beer Aff. ¶ 16, Ex. E)[3]

It was evident that these e-mails were sent using contacts from the Database, as several of the recipients who contacted Verified were people that, although in Verified's Database, have no reason to be solicited by FLO or any other Registered Traveler competitor. (Brill Aff. at ¶ 28; Beer Aff. at ¶ 17.) A prime example is that FLO's e-mails were sent to a good friend — the maid-of-honor — of Verified's Senior Vice President of Corporate Development, Allison Beer. (*Id.*) This friend lives in Canada, has no relation to the aviation, airline, or Registered Traveler industry, FLO, Saflink, or any employer likely to be solicited for the Registered Traveler program in the United States. (*Id.*) Her personal contact information is among the few personal contacts included by Ms. Beer in the Database for her convenience. (*Id.*) There is no legitimate reason why FLO would include her in a solicitation. (*Id.*)

Likewise, defendants' e-mails were received by (a) David Brown, a lawyer in a private law firm whom Verified has retained; (b) Kenneth Klinge, an independent contractor and

[3] These e-mails were sent by a Kevin Mitchell from an entity called the Business Travelers Coalition and indicate that they are on behalf of FLO. On its home page, www.businesstravelcoalition.com, is a link to FLO Corporation's website. (Brill Aff. at ¶ 32, Ex. H (copy of home page for Business Travel Coalition)).

lobbyist for Verified; (c) Vanessa Mazandi, a recent Verified employee; (d) Dick Fogel, a subcontractor for Verified; (e) Mike Lanam, a staffing provider for Verified; (f) Joe Paresi, a subcontractor for Verified; (g) Thomas Flintoft, a lobbyist for Verified; (h) Joe Smith, travel manager for Darden Restaurants, an early Verified corporate customer; (i) Monte Belger, Verified investor and subcontractor; (j) Lori Booker, Verified's public relations contact in Orlando; and (k) Sid Davidoff, Verified's Lobbyist in New York. (Brill Aff. at ¶ 31; Beer Aff. at ¶ 17.) All of these individuals were included on Verified's database. (*Id.*) None of these individuals ever received mailings from Saflink before Fischer started working for FLO. (*Id.*) Each of these individuals independently forwarded the defendants' emails to Verified, to alert it to the issue. (*Id.*) It is obvious that Verified's Salesforce Database is being used to solicit business for FLO.

After Verified's preliminary, internal investigation revealed that Fischer had been attempting to access the Company's Salesforce Database, Verified hired Kroll Ontrack, Inc. to perform a computer forensic analysis to determine the extent of Fischer's intrusion into Verified's system, and to assess and remediate any damage to the system and to implement remedial safeguards to the system, as a result of Fischer's misconduct. Verified has incurred in excess of $5,000 in costs to date in this effort. (Brill Aff. at ¶ 35; Kroll Aff. at ¶ 23.)

ARGUMENT

I. VERIFIED IS ENTITLED TO A TEMPORARY RESTRAINING ORDER AND PRELIMINARY INJUNCTION

A TRO is a provisional remedy intended to prevent the infliction of irreparable injury, and preserve the status quo, until the court can scheduling a hearing on a motion for preliminary injunction. *See* Fed. R. Civ. P. 65(b); 11A Charles A. Wright & Arthur R. Miller, *Federal Practice and Procedure,* § 2951 (1995). To obtain a TRO or a preliminary injunction, the

plaintiff must show (1) irreparable injury absent injunctive relief and (2) either (a) a likelihood of success on the merits or (b) sufficiently serious questions going to the merits and a balance of hardships decidedly tipped in the plaintiff's favor. *N. Atl. Instruments, Inc.* v. *Haber*, 188 F.3d 38 (2d Cir. 1999)(affirming preliminary injunction enjoining former employee from using client list misappropriated from former employer); *see Green Party of N.Y. State* v. *N. Y. State Bd. Of Elections*, 389 F.3d 411, 418 (2d Cir. 2004) (granting request for preliminary injunction); *AIM Int'l Trading, LLC* v. *Valcucine SpA,* 188 F. Supp. 2d 384, 386-87, 388 (S.D.N.Y. 2002)(granting application for temporary restraining order).

Verified has suffered, and will continue to suffer irreparable harm if defendants are not enjoined from soliciting the Database and attempting to hack into Verified's computer systems. Furthermore, Verified has a strong chance of success on the merits, as the evidence demonstrates that Fischer, without authorization and exceeding authorization downloaded Verified's trade secrets and then used them for the benefit of his new employer, Verified's competitor. This unauthorized access and subsequent attempts to hack into the computer system, violates a variety of federal and state laws including the Computer Fraud and Abuse Act, trade secret laws, and is also a breach of Fischer's employment agreement with Verified. Moreover, the balance of hardships tips heavily in favor of Verified, as an injunction merely prevents defendants from profiting from their theft of confidential information and unscrupulous tactics. Indeed, preliminary relief is particularly appropriate in cases, such as this one, where trade secrets are involved, as once disclosed to a competitor, a trade secret can never be recovered. *FMC Corp.* v. *Taiwan Tainan Giant Indus. Co.*, 730 F.2d 61, 63 (2d Cir. 1984)("the loss of a trade secret is not measurable in terms of money damages").

A. Verified Is Likely To Succeed On The Merits Of Its Computer Fraud And Abuse Act Claims

Fischer violated the Computer Fraud and Abuse Act ("CFAA") by accessing and attempting to access Verified's computer systems without authorization, and in excess of any authorization he may have had. The CFAA proscribes both criminal and civil liability for anyone who intentionally "accesses a computer without authorization or exceeds authorized access" where they obtain "information from a protected computer" through interstate communications (18 U.S.C. § 1030(a)(2)(c)), or obtain anything of value in furtherance of an intended fraud (18 U.S.C. § 1030(a)(4)), or where such access or attempted access causes damages. 18 U.S.C. § 1030 (a)(5)(A) and (B).[4]

Fischer violated the CFAA in numerous respects. First, his access to Verified's Salesforce database, after he was terminated, and within the last couple of hours of his employment, was unauthorized and exceeded any authorized access Fischer had to Verified's computer systems. (Brill Aff. at ¶ 10). Indeed, there was no legitimate purpose for such access and for his download of confidential information, nor could there be as Fischer's Employment Agreement unequivocally prohibited his use of Verified's confidential and proprietary information upon termination. (Brill Aff. at ¶ 5, Ex. A.) Nor can there be any question that defendants used this information. As has been demonstrated, numerous contacts from Verified's Salesforce Database received defendants' solicitations, as recently as July 16. Without a doubt, defendants obtained valuable information from Verified's computer systems, and used this information to further their unscrupulous competitive tactics. *See, e.g., Kaufman* v. *Nest Seekers, LLC*, No. 05 Civ. 6782 (GBD), 2006 U.S. Dist. LEXIS 71104, at *25 (S.D.N.Y. Sept. 26, 2006)

[4] "[A]ny person who suffers damage or loss by reason of a violation of this section may maintain a civil action against the violator to obtain compensatory damages and injunctive relief or other equitable relief." 18 U.S.C. § 1030(g).

(employee terminated for cause went to work for competitor and hacked into former employer's computer system); *I.M.S. Inquiry Mgmt. Sys., Ltd. v. Bershire Info. Sys., Inc.*, 307 F. Supp. 2d 521, 531 (S.D.N.Y. 2004) (competitor hacked into plaintiffs' website and retrieved information).

Second, Fischer repeatedly attempted to hack into Verified's systems, well after his employment terminated. The forensic evidence demonstrates that Fischer made at least eight attempts to access the system, most while he was employed as a senior executive at FLO, and in competition with Verified. (Kroll Aff. at ¶¶ 15-22.) *See* 18 U.S.C. § 1030 (a)(5)(B) (noting that liability "in the case of an attempted offense [that] would, if completed, have caused" loss of at least $5,000). Likewise, FLO, Fischer's employer, faces liability for Fisher's recent attempts made while a senior executive of FLO and for FLO's benefit.

Defendants' unauthorized access and hacking attempts have, without question, caused Verified losses in excess of $5,000. (Brill Aff. at ¶ 37; Kroll Aff. at ¶ 23); *See* 18 U.S.C. § 1030(e)(11) (losses include cost of "conducting a damage assessment, and restoring the data, program, system, or information to its condition prior to the offense, and any revenue lost, costs incurred, or other consequential damages incurred because of the interruption of services"); *Nexans Wires S.A.* v. *Sark-USA, Inc.*, 319 F. Supp. 2d 468 (S.D.N.Y. 2004) (loss includes costs associated with investigating damage to computer), *aff'd*, 166 Fed. Appx. 559 (2d Cir. 2006); *E.F. Cultural Travel BV* v. *Explorica, Inc.*, 274 F.3d 577, 585 (1st Cir. 2001)(loss for sums expended to assess whether there was any physical damage to website is not lessened where no actual damage occurred); *Kaufman,* 2006 U.S. Dist. LEXIS 71104 at *25 (investigating damage to computer system may constitute loss).; *I.M.S. Inquiry Mgmt. Sys.,* 307 F. Supp. 2d 521 (damage assessments and remedial measures are recoverable losses under the CFAA).

B. Verified Is Likely To Prevail On The Merits Of Its Misappropriation Of Trade Secrets Claim

To succeed on a claim for misappropriation of trade secrets a plaintiff must demonstrate that (1) it possessed a trade secret and (2) the defendants used the trade secret in breach of an agreement, confidential relationship or duty, or as a result of discovery by improper means. *N. Atl.*, 188 F.3d at 43-44 (affirming injunction) citing *Hudson Hotels Corp.* v. *Choice Hotels Int'l*, 995 F.2d 1173, 1176 (2d Cir. 1993)). Defendants misappropriated Verified's trade secrets from its Salesforce Database.

1. Verified's Customer Accounts Constitute Protectable Trade Secrets

The contact information that defendants misappropriated from the Salesforce Database is precisely the type of valuable information that courts deem protectable trade secrets. *See, e.g., N. Atl.*, 188 F.3d at 44 (finding customer lists were trade secrets); *B.U.S.A. Corp. v. Ecogloves, Inc.*, No. 05 Civ. 9988 (SCR), 2006 U.S. Dist. LEXIS 85988, at * 11 (S.D.N.Y. Jan. 31, 2006) (although company names that advertise their locations publicly are not trade secrets, the names of "specific contacts at those companies are")(*citing N. Atl.,* 188 F.3d at 44-45).

A trade secret is "any formula, pattern, device or compilation of information which is used in one's business, and which gives [the owner] an opportunity to obtain an advantage over competitors who do not know or use it." *Softel, Inc.* v. *Dragon Med. & Scientific Commc'ns, Inc.*, 118 F. 2d 955, 968 (2d Cir. 1997) (*quoting* Restatement of Torts § 757 cmt. b (1939). New York courts evaluate trade secrets on the basis of the following six factors:

> (1) the extent to which the information is known outside of the business; (2) the extent to which it is known by employees and others involved in the business; (3) the extent of measures taken by the business to guard the secrecy of information; (4) the value of the information to the business and its competitors; (5) the amount of effort or money expended by the business in developing the information; and (6) the ease or difficulty with which the information could be properly acquired or duplicated by others.

Ashland Mgmt. Inc. v. *Janien*, 82 N.Y.2d 395, 407, 604 N.Y.S.2d 912, 917 (1993) (quotations and citations omitted). Verified's contacts within the Salesforce database fall squarely within these factors.

Verified's Salesforce Database is not publicly known. This is not merely a list of contacts that could be found in a public directory. Instead, the Database contains specific information pertaining to each contact, each of whom is a crucial player in the complex decision-making process of airport authorities and other strategic partners. (Brill Aff. at ¶¶ 7-8; Beer Aff. at ¶¶ 2-5.). This information cannot be found simply by searching the web. *See, e.g., B.U.S.A.*, 2006 U.S. Dist. LEXIS, at * 9-10 (personal contacts were trade secrets because they could not be found easily on the websites of potential customers). Verified has spent four years collecting and compiling this information, which has great value to Verified's competitors precisely because it provides a roadmap to the potential decision makers in airports and with potential strategic partners; and because it constitutes information not generally known to Verified's competitors. (*Id.*) *See N. Atl.*, 188 F.3d at 44 ("[a] customer list developed by a business through substantial effort and kept in confidence may be treated as a trade secret and protected at the owner's instance against disclosure to a competitor, provided the information it contains is not otherwise readily ascertainable."). Indeed, even if defendants invested similar time and effort to replicate this information, it is unlikely they could duplicate this compilation to the extent Verified's list is the product of its particular understanding of the industry it pioneered, and how business decisions are made in that industry. (Brill Aff. at ¶¶ 2, 7-8.) Moreover, notes and comments as to particular negotiations and deals constitute information that in no stretch of the imagination could be deemed public. (*Id.* at ¶ 7.)

Verified has also engaged in substantial efforts to maintain the confidentiality and security of its contact information within the Salesforce Database. These efforts include:

(1) limiting access to only key executive employees (Brill Aff. at ¶ 7; Beer Aff. at ¶ 7); (2) obtaining signed employment agreements, including from Fischer, expressly setting forth employee obligations to maintain the confidentiality of such information (*Id*; Brill Aff. at ¶ 5); (3) establishing policies and procedures, as set forth in the employee handbook, which clearly alerted employees that Verified took the confidentiality of its trade secrets seriously, proclaiming that it would "fire anyone who reveals any of this without authorization" (Brill Aff. at ¶ 6); (4) providing continuous reminders from senior management of the employee's obligation to maintain the confidentiality of Verified's trade secrets (Beer Aff. at ¶ 9; Brill Aff. at ¶ 8); (5) instituting password restricted terminals and websites (Beer Aff. at ¶ 8); and (6) maintaining an electronic log of all attempts to access the Salesforce Database. (*Id.*)

Indeed, Fischer's Employment Agreement expressly obligated him to maintain the confidentiality of Verified's trade secrets, for "five years" beyond the term of his employment. (Employment Agreement at 2.) *See, e.g., N. Atl.*, 188 F.3d at 45 (district court properly determined existence of trade secret on basis, in part, that the "Employment Agreement itself … requiring that [defendant] 'keep secret and retain in the strictest confidence all confidential matters … including … customer lists….'"). In consideration, Fischer was highly compensated. (Brill Aff. at ¶ 5.)[5]

2. Fischer Misappropriated Verified's Trade Secrets

New York law imposes a duty not to use trade secrets in competition with a former employer. *Hudson Hotels*, 995 F.2d at 1176. In this case, this duty is reinforced by Fischer's Employment Agreement. (Brill Aff., Ex. A) "[A]n agent has a duty not to use confidential

[5] A redacted version of the Employment Agreement, removing Fischer's salary, is attached as Exhibit A to the Brill Affidavit. An unredacted version will be provided to the Court at oral argument.

knowledge acquired in his employment in competition with the principal," and this duty "exists as well after the employment is terminated as during its continuance." *N. Atl.*, 188 F.3d at 47 (*quoting ABKCO Music Inc.* v. *Harrisongs Music, Ltd.,* 722 F.2d 988, 994 (2d Cir. 1983) (internal citations and quotations omitted). Although this duty is implied in every employment contract, Fischer and Verified expressly provided for a duty to maintain the confidentiality of Verified's trade secrets for five years after termination. (Brill Aff., Ex. A) *See N. Atl.*, 188 F.3d at 45 (enforcing similar confidentiality provision).

Fischer is required to keep Verified's trade secrets "strictly confidential," which, not surprisingly, precludes "using that confidential information for the benefit of a competitor business." *N. Atl.*, 188 F.3d at 48 (finding that defendant misappropriated trade secrets). Yet, that is precisely what Fischer did here. Incredibly, on his last day of work at Verified, Fischer brazenly stole confidential information from the Salesforce Database, and has used it to benefit FLO and Saflink by, among other things, repeatedly soliciting Verified's contacts. In addition, he made no less than eight attempts to hack into Verified's systems, no doubt to steal more trade secrets.

3. FLO And Saflink Misappropriated Verified's Trade Secrets

A claim for misappropriation of trade secrets also lies where a defendant used the trade secret "as a result of discovery by improper means." *Hudson Hotels*, 995 F.2d 1173, 1176 (2d Cir. 1993). "Discovery by improper means" does not require that the defendant himself breach a duty. Instead, it merely requires that the defendant "discloses or uses another's trade secret" that was learned "from a third person with notice . . . that it was secret and that the third person discovered it by improper means or that the third person's disclosure of it was otherwise a breach of his duty to another." *Anacomp, Inc.* v. *Shell Knob Servs.*, No. 93 Civ. 4003 (PKL), 1994 U.S.

Dist. LEXIS 223, at *40-41 (S.D.N.Y., Jan. 7, 1994), *quoting Computer Assocs. Int'l, Inc.* v. *Altai Inc.*, 982 F.2d 693 (2d Cir. 1992), (*quoting Restatement of Torts* § 757)).

FLO and Saflink were well-aware of Fischer's previous employment with Verified and his unscrupulous tactics. (Brill Aff. at ¶¶ 16-27.) Indeed, Fischer's disclosure of Verified's trade secrets was a key subject during the resolution of the previous litigation between the parties, and FLO's president proclaimed that they would "control him." (Brill Aff. at ¶ 27.) But, instead, defendants used Verified's trade secrets for their benefit, making several solicitations on Saflink's and FLO's behalf. (Brill Aff. at ¶¶ 28-33; Beer Aff. at ¶¶ 11-14.)

C. Fischer Breached His Employment Agreement With Verified

Fischer's breach of the written Employment Agreement and its confidentiality provision provides the Court with an independent basis for issuing injunctive relief. The contract expressly provides for "equitable relief" in the event of a breach. (Brill Aff., Ex. A) *See, e.g., Murphy Door Bed Co.* v. *Interior Sleep Sys., Inc.*, 874 F.2d 95, 102-03 (2d Cir. 1989)(notwithstanding invalid trademark, injunctive relief was proper and awarded based on contractual rights). Fischer's unauthorized computer access, theft of Verified's trade secrets, and use of those trade secrets demonstrate a clear violation of his contractual obligations to maintain the confidentiality of Verified's confidential information.[6]

[6] Verified is also likely to prevail on its other claims asserted in the Complaint: conversion (Count V; *see Thyroff v. Nationwide Mutual. Insurance Co.*, 8 N.Y.3d 283, 832 N.Y.S.2d 873 (2007) for unlawful conversion of Verified's electronic data); tortious interference with contract (Count IV; *see World Wrestling Federation Entertainment, Inc.* v. *Bozell*, 142 F. Supp. 2d 514, 532 (S.D.N.Y. 2001) for maliciously interfering with Verified's Employment Contract with Fischer); and violations of New York's General Business Law, Section 349(h) (Count VI, *Magnalock Corp. v. Schnabolk*, 65 F.3d 256 (2d Cir. 1995)for deceptive practices).

D. Verified Will Suffer Irreparable Injury Absent The Granting Of Preliminary Relief

While the actual and threatened loss of trade secrets alone constitutes irreparable harm for any company, the harm to Verified is all the more acute because the Salesforce Database provides a crucial advantage in this emerging industry. (Brill Aff. at ¶ 2, 8.) It is well settled that the theft of confidential business information, including trade secrets, is irreparable and worthy of protection by injunctive relief. *See, e.g., Johnson Controls, Inc.* v. *A.P.T. Critical Sys., Inc.*, 323 F. Supp. 2d 525, 532 (S.D.N.Y. 2004)("Irreparable harm to an employer may also result where an employee has misappropriated trade secrets or confidential customer information, including … customer lists and customer preferences."); *Computer Assocs. Int'l, Inc.* v. *Bryan,* 784 F. Supp. 982, 986 (E.D.N.Y. 1992) (for purposes of a motion for a preliminary injunction, loss of trade secrets is not measurable in terms of money damages and it thus considered irreparable) (*quoting FMC Corp.* v. *Taiwan Tainan Giant Indus., Co.*, 730 F.2d 61, 63 (2d Cir. 1984)("the loss of a trade secret is not measurable in terms of money damages") (internal quotations omitted); *Stanley Tulchin Assocs. v. Vignola*, 186 A.D.2d 183, 185, 587 N.Y.S.2d 761, 762 (2d Dep't 1992)(holding that plaintiff's client list containing names and telephone numbers of clients, contacts, and the value of business done with the clients were of the type of information covered by a non-disclosure provision and subject to protection by injunction).

Indeed, it is also clear that the threatened loss of business – as is the case here -- can constitute irreparable harm. *See Johnson Controls*, 323 F. Supp. 2d at 532 ("it is very difficult to calculate monetary damages that would successfully redress the loss of a relationship with a client that would produce an indeterminate amount of business in the years to come") (citations and quotations omitted).

Verified pioneered this industry, and the emerging nature of the industry underscores the competitive importance the Company places on its trade secrets. (Brill Aff. at ¶¶ 2-3, 8.) Verified's success depends on its ability to maintain the confidentiality of this information. (*Id.*) If Verified is not granted preliminary relief, it will suffer immediate and irreparable injury, as the defendants, notably Fischer, have already evidenced their unscrupulous behavior by using and disclosing the Company's protected information to unfairly compete. Indeed, even after Verified's CEO contacted FLO's president to discuss Fischer's misconduct, less than a week later another e-mailing was sent out to Verified's contacts. (Brill Aff. at ¶ 32; Beer Aff. at ¶ 15.) *See also Ecolab* v. *Paolo*, 753 F. Supp. 1100 (E.D.N.Y. 1991)("[l]oss of good will constitutes irreparable harm. The use and disclosure of an employer's confidential customer information and the possibility of loss of customers through such usage constitutes irreparable harm.") (citations omitted).

A failure to award preliminary relief in this case would essentially transfer Verified's protected property—developed at its great expense—to its direct competitor, who has so far been unable to succeed in competing with Verified. It is clear that FLO only learned of this information as a result of Fischer's employment at Verified, his unlawful access to Verified's computers, and defendants' subsequent misappropriation of the confidential information.

Under these circumstances, the loss to Verified, and unfair gain to defendants, will likely be impossible to determine, and there is no adequate remedy at law for Verified. *N. Atl.,* 188 F.3d at 49 (affirming preliminary injunction and holding that "loss of trade secrets cannot be measured in money damages") *(quoting FMC Corp.*, 730 F.2d at 63.) Indeed, in his Employment Agreement, Fischer agreed to maintain the confidentiality of Verified's trade secrets and agreed that "any violation of this provision shall be subject to equitable relief." (Brill Aff. Ex. A at 2.)

E. The Balance Of Hardships And The Public Interest Tip Decidedly In Favor Of Granting An Injunction

At a minimum, the affidavits submitted in support of Verified's application, as detailed above, raise sufficiently serious questions as to the merits of this action. In that event, the balance of equities weigh heavily in favor of granting an injunction. Weighed against the years of effort that Verified has invested in the compilation of its customer accounts and other confidential information, the harm suffered by Verified if the relief is not granted is overwhelmingly greater than any harm defendants could conceivable suffer from an injunction preventing the use of Verified's trade secrets and prohibiting future computer hacking. (Beer Aff. at ¶¶ 14-18; Brill Aff. at ¶¶ 7-8.) The public has a strong interest in enjoining anyone from using stolen confidential trade secrets. There is an equally compelling public interest in preventing defendants from unlawfully using information confidentially compiled and obtained by Verified to wholesale solicit individuals whose contact information would otherwise be beyond defendants' reach. (Beer Aff. at ¶ 17; Brill Aff. at ¶ 28-32.)

II. VERIFIED SHOULD BE GRANTED EXPEDITED DISCOVERY

Rule 26 of the Federal Rules of Civil Procedure authorizes the Court to grant expedited discovery upon the more "flexible" standards of "reasonableness" and "good cause." *Ayyash* v. *Bank Al-Madina*, 233 F.R.D. 325, 326-27 (S.D.N.Y. 2005)("employing a preliminary-injunction type analysis to determine entitlement to expedited discovery makes little sense, especially when applied to a request to expedite discovery in order to prepare for a preliminary injunction hearing"). Good cause exists when discovery is needed in connection with an application for TRO or preliminary injunction, even when made on an *ex parte* basis. *Id.* at 327 (plaintiff granted expedited discovery *ex parte* against third parties). Moreover, the "need for discovery" is all the more urgent when "defendants are now aware of the action (and thus have an incentive

to conceal assets)." *Id.* See *also* W. Schwarzer, A.W. Tashima, J. Wagstaffe, *Federal Civil Procedure Before Trial* § 11:157 (1993) (Federal Rules of Civil Procedure require a court order if plaintiff desires to take a deposition during the first 30 days after service of the summons and complaint, and "good cause [for such an order] may exist because of the urgent need for discovery in connection with an application for TRO or preliminary injunction") (internal quotations omitted).

Defendants' misconduct was, as far as plaintiff is aware, conducted via electronic means. Consequently, defendants are possibly in possession of highly relevant evidence establishing the details of their breach or, worse, additional breaches via electronic or other means. Moreover, expedited discovery is also required to establish the full extent of defendants' breaches so that Verified can quickly undertake to remedy any harm.

CONCLUSION

Defendants' theft, use and disclosure of Verified's confidential information and other misconduct detailed above, entitles plaintiff to, among other things, injunctive relief. Defendants and their agents should be required to immediately return or certify the destruction of all confidential or proprietary Verified information. In addition,defendants and their agents should be enjoined from (1) soliciting for business, or making sales to, any and all individuals and corporations affiliated with individuals whose contact or other information was contained in plaintiff's Salesforce Database for a period of 6 months; (2) using, disclosing, misappropriating or otherwise utilizing plaintiff's proprietary or confidential information; and (3) disparaging Verified to any third party. In addition to this relief, Verified is also entitled to any other relief this court deems just and proper.

Dated: New York, New York
July 19, 2007

MORRISON & FOERSTER LLP

By: _____

Jamie A. Levitt
Damion K.L. Stodola
1290 Avenue of the Americas
New York, New York 10104
(212) 468-8000
Attorneys for Plaintiff Verified Identity Pass, Inc.

Of Counsel:

Lori A. Schechter
MORRISON & FOERSTER LLP
425 Market Street
San Francisco, California 94105-2482
(415) 268-7000